Penyandian Teks Dengan Metode *Hill Chiper*

Pratiwi Rachmadi
Teknik Informatika, Fakultas Teknologi Informasi Perbanas Jakarta
Jl Perbanas Karet Kuningan Setiabudi Jakarta 12940
wiek.pratiwi@gmail.com; pratiwi@perbanas.id

Abstrak

Perkembangan teknologi informasi saat ini secara tidak langsung mempengaruhi bidang komunikasi data. Saat ini banyak aplikasi komunikasi yang terkait dengan data, maka perlu dikhawatirkan keamanan data itu sendiri. Keamanan data menjadi sangat penting dan menjadi perhatian terutama pada obyek yang terkait masalah ekonomi keuangan dan perbankan. Pada penelitian ini dilakukan untuk enkripsi dan dekripsi pada teks berupa PIN (Personal Identifier Number) yang diterima nasabah perbankan ketika menerima kartu ATM atau kartu kredit. Studi ini mencoba untuk menjaga agar pesan berupa PIN tersampaikan dengan baik dan aman. Untuk melakukan pengkodean ini dilakukan dengan menggunakan algoritma kriptografi Hill Chiper. Diperoleh hasil yang sempurna untuk 10 data PIN dengan kunci K yang sama pada penelitian ini.

Kata kunci*: Kriptografi, Hill Chiper, Personal Identifier Number*

Abstract

The development of information technology today indirectly affect the field of data communication. Currently many communication applications related to the data, it is necessary to worry about the security of the data itself. Data security becomes very important and a concern especially on the objects related to financial and banking economic issues. In this research is done for the encryption and decryption in text in the form of PIN (Personal Identifier Number) accepted by banking customer when accept ATM card or credit card. This study tries to keep messages in the form of PINs delivered properly and safely. To perform this encoding is done by using Hill Chiper cryptography algorithm. The results obtained are perfect for 10 PIN data with the same K key .

Keyword: *Cryptography, Hill Chiper, Personal Identifier Number*

1. Pendahuluan

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, namun sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Apabila terjadi gangguan terhadap keamanan data yang dimiliki maka para pengelola dan pengguna memperhatikan dengan seksama. Berbagai macam teknik digunakan dalam upaya mengamankan suatu data penting. Sebelumnya telah ada cara untuk menjaga keamanan data yang dikenal dengan nama kriptografi. Dengan kriptografi data rahasia terjaga keamanannya, namun bentuk *chipertext* yang diacak akan mudah terdeteksi dan menyadarkan pihak ketiga akan kerahasiaan file tersebut. Untuk itu diterapkan steganografi(*covered writing*) dalam usaha menjaga kerahasiaan data.

Pengamanan data dan dokumen adalah sangat penting, dan harus dilakukan dengan baik. Pada *Hill Cipher*, media gambar dipergunakan untuk menyembunyikan pesan rahasia [1][2]. Proses pengiriman pesan teks pada gambar dengan format JPEG akan disisipkan dengan pesan teks yang telah dienkripsi, setelah itu gambar yang telah tersisipi pesan teks akan dikirimkan. Kombinasi antara steganografi dengan kriptografi dilakukan apabila gambar yang berisi pesan yang telah disisipkan diketahui isinya, sehingga dengan adanya kriptografi pesan yang telah diketahui isinya tidak secara pasti dapat dibaca karena masih berupa cipherteks yang memerlukan kunci untuk dapat membaca kembali isi pesan yang sebenarnya (plainteks).

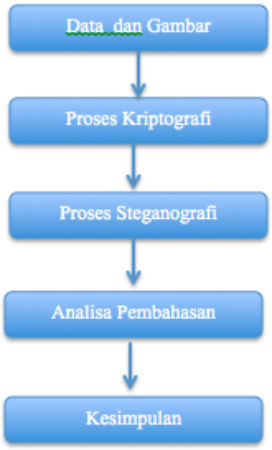
Berkembangnya teknologi disegala bidang juga di bidang perbankan maka akan terdapat banyak kemudahan. Namun dibalik itu kewaspadaan meningkatkan keamanan harus diperhatikan terutama pada transaksi perbankan. Transaksi perbankan meliputi produk tabungan, giro, deposito, kredit tentu saja memerlukan keamanan dalam transaksinya. Dalam melakukan transaksi pada saat ini transaksi perbankan untuk produk perbankan seperti

tabungan dan kartu kredit dilengkapi dengan kartu dan di dalam kartu tersebut terdapat PIN (Personal Identifier Number) untuk mengidentifikasi keabsahan pemilik kartu. Faktor keamanan menjadi sangat penting untuk menjada kerahasiaan data ini. Atas dasar itu penulis melakukan penelitian bagaimana melakukan penyandian teks, dalam hal ini PIN nasabah dengan menggunakan metode *Hill Chiper*.

2. Metode Penelitian

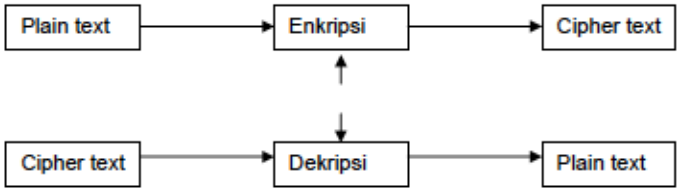
Data digunakan pada penelitian ini adalah teks berupa angka yang mewakili PIN yang dikirmkan oleh Bank kepada nasabah. Teks PIN berupa 6 digit angka yang digunakan sebagai password dalam penggunaan kartu ATM atau kartu kredit dari Bank. Pada teks ini dilakukan proses kriptografi yaitu penyandian pada teks pin 6 digit dengan menggunakan metode Hills Chiper dengan teknik perkalian matriks dan teknik invers terhadap matriks. Teks yang sudah terenkripsi ini disisipkan ke dalam gambar yang mewakili identitas pemberi PIN seperti logok bank atau yang lainnya. Nasabah dapat mengetahui teks asli maka dilakukan dekripsi pada PIN tersebut. Baik pada proses enkripsi dan dekripsi pada penelitian ini dilakukan dengan metode Hill Chiper.

Proses selanjutnya adalah steganografi yaitu suatu ilmu dan seni menyembunyikan data pada suatu media. Data yang akan disembunyikan adalah teks berupa pin 6 digit tersbut ke dalam gambar berupa logo dari bank penerbit kartu ATM atau Kartu kredit. Steganografi tercipta sebagai salah satu cara yang digunakan untuk mengamankan data dengan cara menyembunyikannya dalam media lain agar “tidak terlihat”. Untuk menyembunyikan pesan dalam gambar tanpa mengubah sifat yang terlihat, media penutup dapat diubah di dalam wilayah "*noisy*" dengan variasi warna yang lebih banyak, sehingga lebih sedikit perhatian pada daerah modifikasi tersebut. Metode yang paling umum digunakan pada media gambar adalah dengan *Least Significant Bits* atau LSB [3].



Gambar 1. Penelitian besar yang dilakukan

Pada proses kriptografi dengan metode Hill Chiper yang dilakukan adalah enkripsi dan dekripsi pada obyek berupa PIn yang mengikuti proses seperi pada gambar 2.



Gambar 2. Proses kripografi pada teks dalam penelitian.

Obyek penelitian pada proses kriptografi penelitian ini adalah PIN maka data yang digunakan berupa angka yang diwakili oleh tabel 1. Teks berupa angka yang ada pada PIN di enkripsi dengan metode *Hil Chiper.*

Tabel1. Kode ASCII untuk angka 0-9 yang digunakan dalam pin kartu ATM

48	0
49	1
50	2
51	3
52	4
53	5
54	6
55	7
56	8
57	9

Memasukkan teks ke dalam gambar dengan data yang diproses berupa karakter (string). Dalam melakukan enkripsi dan dekripsi hill cipher terhadap record dengan panjang karakter yang dienkripsi. Dasar dari teknik *Hill Cipher* adalah aritmatika modulo terhadap matrik. Dalam penerapannya, *Hill Cipher* menggunakan teknik perkalian matrik dan teknik invers terhadap matrik. Kunci pada *Hill Cipher* adalah matriks n x n dengan n merupakan ukuran blok. Matrik K yang menjadi kunci harus merupakan matriks yang *invertible*, yaitu memiliki *multiplicative inverse* K^{-1} sehingga : K . K^{-1} = 1. Kunci harus memiliki invers karena matriks K^{-1} tersebut adalah kunci yang digunakan untuk melakukan dekripsi.

$$K = \begin{pmatrix} k_{11}\, k_{12} \ldots k_{1n} \\ k_{21}\, k_{22} \ldots k_{2n} \\ \ldots \ldots \ldots \ldots \\ k_{m1}\, k_{m2} \ldots k_{mn} \end{pmatrix}$$

Gambar 2. Matrik K sebagai kunci pada proses enkripsi

3. Hasil dan Pembahasan

Data yang dipakai pada penelitian ini digunakan kombinasi angka secara acak 6 digit pin yaitu :

1) 234567
2) 459034
3) 789023
4) 789090
5) 890824
6) 808342
7) 990909
8) 890223
9) 234108

Sebuah blok dari n huruf dinyatakan sebagai vektor dimensi n, dan dikalikan dengan matriks nxn, modulo 26. Komponen matriks merupakan kunci, dipilih random dengan syarat merupakan matriks invertibel untuk memastikan bahwa dekripsi mungkin dilakukan. Misalnya diambil sebuah kunci matriks berukuran 6x6.

$$\begin{pmatrix} 1 & 6 & 24 & 3 & 1 \\ 3 & 6 & 4 & 6 & 3 \\ 21 & 8 & 6 & 1 & 1 \\ 4 & 13 & 16 & 4 & 10 \\ 5 & 10 & 17 & 0 & 15 \end{pmatrix}$$

Maka akan di enkripsi pesan 234567 dengan 2= 50, 3= 51, 4= 52, 5=53,6= 54, 7 = 55

$$\begin{pmatrix} 1 & 6 & 24 & 3 & 1 \\ 3 & 6 & 4 & 6 & 3 \\ 21 & 8 & 6 & 1 & 1 \\ 4 & 13 & 16 & 4 & 10 \\ 5 & 10 & 17 & 0 & 15 \end{pmatrix} \begin{pmatrix} 50 \\ 51 \\ 52 \\ 53 \\ 54 \\ 55 \end{pmatrix} = \begin{pmatrix} 23 \\ 24 \\ 25 \\ 26 \\ 27 \\ 28 \end{pmatrix} \text{ mod } 26$$

$$\begin{pmatrix} 23 \\ 24 \\ 25 \\ 26 \\ 27 \\ 28 \end{pmatrix}$$

Matrik dikonversi menjadi pesan ETB CAN EM SUB ESC FS

Untuk mendeskripsikan pesan kembali maka dicari inver modulo 26 dari matrik kunci

$$\begin{pmatrix} 1 & 6 & 24 & 3 & 1 \\ 3 & 6 & 4 & 6 & 3 \\ 21 & 8 & 6 & 1 & 1 \\ 4 & 13 & 16 & 4 & 10 \\ 5 & 10 & 17 & 0 & 15 \end{pmatrix} \text{ diperoleh matrik } \begin{pmatrix} 1 & 6 & 24 & 3 & 1 \\ 3 & 6 & 4 & 6 & 3 \\ 21 & 8 & 6 & 1 & 1 \\ 4 & 13 & 16 & 4 & 10 \\ 5 & 10 & 17 & 0 & 15 \end{pmatrix}$$

Pesan yg diterima yaitu “ETB CAN EM SUB ESC FS” di kembalikan/deskriptif ke pesan semula sehingga diperolen pin 2 3 4 5 6 7 kembali.
Proses yang sama dilakukan pada 9 angka PIN yang lainnya dan diperoleh data awal sebelum dilakukan enkripsi dan dekripsi dengan tingkat keberhasilan 100% dengan menggunakan matrik K sebagai kunci yang sama.

4. Kesimpulan

Pada kriptografi, proses menyandikan text (password) dilakukan dengan metode Hill berjalan dengan baik untuk 6 digit angka pada PIN (Personal Identifier Number) yang diberikan oleh bank kepada nasabahnya. Implementasi cipher hills pada kode ASCII memberikan kemungkinan yang luas pada lebih banyak karakter yang tercakup, tidak hanya terbatas pada 26 alfabet, tetapi juga mencakup karakter-karakter seperti . ,”, ‘,=,@,#,% dan sebagainya. Disarankan dilakukan penelitian dengan lebih beragam kunci K untuk memperoleh keamanan yang optimal pada proses kriptografi dengan metode ini.

Referensi

[1.] Acharya B, (2009). *Image Encryption Using Advanced Hill Cipher Algorithm*, Research Paper International Journal Of Recent Trends In Engineering, Vol. 1, No. 1

[2.] Abdul Halim Hasugian, (2013). Implementasi Algoritma Hill Cipher Dalam Penyandian Data , Pelita Informatika Budi Darma, Volume IV no 2

[3.] Alatas Putri, M. Subali, (2009). *Implementation Technique With Steganography LSB Method in Digital Images*, Undergraduate Program, Faculty of Computer Science, Gunadarma University

[4.] Budi Raharjo, (2002). *Keamanan Sistem Informasi Berbasis Internet*, PT Insan Infonesia Bandung & PT INDOCISC – Jakarta

[5.] Hondro ,Rivalri Kristianto, (2006. *Aplikasi Enkripsi Dan Dekripsi Sms Dengan Algoritma Zig Zag Cipher Pada Mobile Phone Berbasis Android*

[6.] JJ Siang dan Ronald S Laser, (2002). *Implementasi Sandi Hill Untuk Penyandian Citra*, Journal informatics Petra vol 3, no 1

[7.] Rohayah S, Sasmito G.W, Somantri O, (2015). *Aplikasi Steganografi Untuk Penyisipan Pesan* , Jurnal Informatika Vol. 9, No. 1

[8.] Schneier, (2000). *An Introduction Cryptography*, e book Copyright © 1990–2000 Network Associates, Inc. and its Affiliated Companies